

홈네트워크 시스템의 양방향 기기 인증 메커니즘에 관한 연구

A Study on interactive device authentication mechanism
in the home network system

백상준, 이성진, 배성호, 오세웅*
동명정보대학교, 동의대학교*

Baek Sang-Joon, Lee Sung-Jin, Bae Sung-Ho,
Oh Sei-Wong*

Tongmyong University of Information and
Technology Donggeui University*

요약

기존 유선 방식의 홈네트워크 시스템에 무선 방식이 적용됨에 따라 사용자들은택내 어디에서나 편리하게 홈네트워크 서비스를 이용할 수 있게 되었다. 이러한 홈네트워크 시스템에서 안전한 네트워크를 구성하기 위해서는 사용자의 인증과 더불어 무선을 사용하는 기기들에 대한 양방향 인증이 필요하다. 본 논문에서는 안전한 무선 홈네트워크 환경을 구축하기 위한 양방향 인증 메커니즘을 제안한다.

Abstract

Applying wireless mode to an existing wired home network system, the users became to use services of home network conveniently in their home. In order to construct a safe network in home network system, it needs user authentication and interactive authentication to mobile devices. In this paper, we propose an interactive authentication mechanism in order to make a safe home network system in mobile environment.

I. 서론

홈네트워크(Home network)는 가정 내의 모든 정보가전기기가 유무선 네트워크로 연결되어 누구나 시간, 장소에 구애 받지 않고 다양한 디지털 홈서비스를 제공받을 수 있는 미래지향적인 가정환경을 제공한다. 이로 인해 정보차별의 격차가 점점 해소되고 보다 나은 삶의 환경을 누릴 수가 있게 되었다. 홈네트워크 도입과 더불어 가정에서 사용하는 가전기기들의 디지털화, 네트워크화 및 지능화 추세가 두드러져 향후 정보가전기기로 도입 될 추세가 더욱 증가할 것으로 보인다. 이러한 정보가전기기로 홈네트워

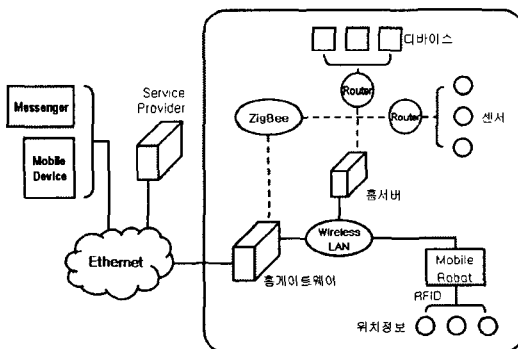
크를 구성함에 있어 사용자들의 편의성과 설비에 대한 번거러움을 해소하기 위해 홈네트워크를 무선으로 구성하고 있다. 그러나 무선 기반의 홈네트워크 시스템에서는 개인정보나 제어정보 등이 공중을 통하여 전달되기 때문에 해킹이나 스니핑 등의 방법을 통한 홈네트워크에 침입이 가능하다. 그래서 무선 홈네트워크는 보안 대책이 수립 되어야 한다. 무선 홈네트워크의 보안은 두 가지 관점에서 볼 수 있다. 첫째는 오고가는 데이터를 제 삼자가 알지 못하도록 하는 암호화에 관한 것이고, 둘째는 무선 네트워크 기기 간에 서로 올바른 상대에게 정보를 보내고 있는지에 대한 기기 인증에 관한 것이다. 이러한 방법들은

사용자에 의해 아이디나 패스워드를 입력해야 하는 경우가 많고 사용자 입력 인터페이스가 없는 기기들에게는 아이디와 패스워드로 인증하는 방식을 기기로 강구해야 한다. 또한 미래 고령화 사회에서는 이러한 입력 절차들이 홈네트워크를 편리하게 사용하는데 많은 불편을 가져 올 수 있다. 기존의 연구들은 이러한 문제를 고려하지 않은 아이디와 패스워드 기반의 사용자 인증이나 인증서 기반의 기기 간 인증 절차가 많았다.[2][6]

본 논문은 이러한 문제점에 대한 방안으로 홈네트워크 시스템의 홈게이트웨이[5]와 기기 간에 인증을 위한 중계 역할을 하는 모바일 로봇(Mobile Robot)[8], 그리고 기기의 정보를 가지고 있는 RFID(Radio Frequency Identification)[7]를 이용한 양방향 자동 기기 인증 메커니즘을 제안하고 설계한다. RFID를 이용하여 사용자는 번거로운 입력 절차도 거치지 않고 정보가전기기들을 더욱 편리하게 인증할 수 있도록 하였으며, RFID 태그 내에 저장된 맥 어드레스 정보를 관리함으로써 홈게이트웨이와 기기 간에 보다 안전한 홈네트워크를 구축 할 수 있도록 설계하였다.

II. 메커니즘 설계

1. 전체 홈네트워크 시스템



▶▶ 그림 1. 홈네트워크 시스템 구성도

그림 1은 본 논문에서 제안한 메커니즘이 적용될 무선 홈네트워크의 전체 시스템 구성도이다. 이 시스템은 사용자의 인터페이스 역할을 수행하는 모바일 로봇, OSGi(Open Service Gateway Initiative) 플랫폼과 UPnP(Universal Plug and Play)[1]를 이용하여 맥내의 정보가전기기들을 제어, 관리 하는 홈게이트웨이, 맥내의 대용량 멀티미디어 데이터(multimedia data)를 저장·관리하는 홈서버 그리고 UPnP를 지원 하는 기기와 다양한 센서(sensor)들로 구성된다.

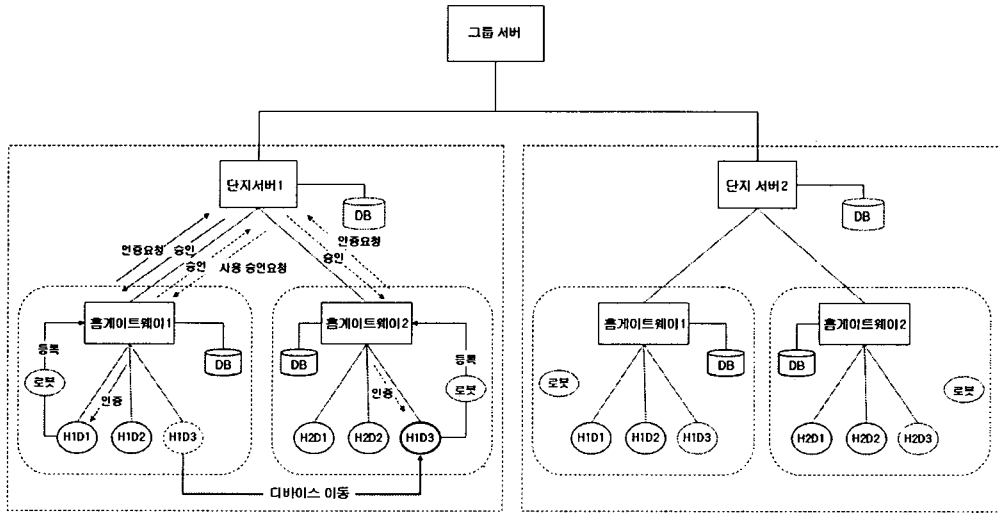
본 메커니즘이 적용될 무선 홈네트워크 시스템은 대용량, 초고속 데이터 전송에 적합한 무선랜[3] 기술과 정보가전기기의 제어 및 홈오토메이션에 적합한 직비(ZigBee)[4] 기술을 사용하여 무선 환경을 구성한다. 또한 모바일 로봇을 적용시킴으로써 기기 인증 등의 보안 문제를 해결할 수 있으며 최적화된 인터페이스(interface)를 통해서 간편한 제어가 가능하다. 홈게이트웨이와 모바일 로봇은 무선으로 연결이 되어있으며 두 기기 간에는 인증과 암호화가 이루어져 안전한 채널이 형성되어 있고 이를 이용하여 무선 정보가전기기들을 홈네트워크에 참여시킬 수 있다.

2. 인증 메커니즘

2.1. 전체 인증 메커니즘

그림 2는 기기의 인증을 설명하기 위한 전체 인증 메커니즘 구성도이다. 그림 1에서 나타낸 바와 같이 맥내에서 새로운 가전기기를 사용하기 위하여 모바일 로봇을 이용해 기기에 대한 정보를 홈게이트웨이에 등록을 하고 홈게이트웨이는 자신의 정보를 추가해서 단지 서버에 기기를 등록을 하게 된다. 그리고 무선 홈네트워크에서는 양방향 인증이 이루어져야 하기 때문에 기기에서도 홈게이트웨이에 대한 인증이 필요하다.

홈네트워크1에서 사용하던 기기를 홈네트워크2에서 사용하기 위해서 홈게이트웨이2는 홈게이트웨이1로부터 사용 승인을 받아야한다. 즉 이 기기는 홈게

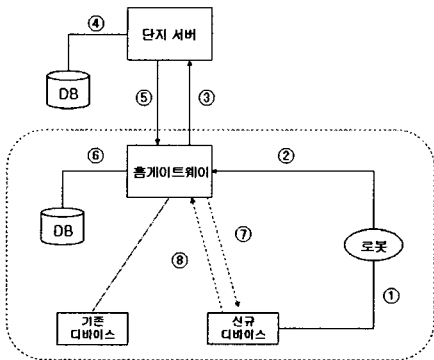


▶▶ 그림 2. 전체 인증 메커니즘 구성도

이트웨이1의 기기로서 단지 서버에 등록이 되어 있는 상태이고 홈게이트웨이2에서는 신규 기기로서 단지 서버로 등록을 하게 되며 단지 서버는 홈게이트웨이1에게 기기 사용승인 요청을 하여 승인을 받은 경우에 홈게이트웨이2에게 승인 후 사용이 가능하게 해준다.

2.2 양방향 자동 기기 인증

그림 3은 새로운 기기와 홈게이트웨이간의 양방향 자동 기기 인증을 보여주기 위한 메커니즘 구성도이다.

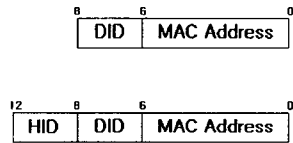


▶▶ 그림 3. 양방향 자동 기기 인증 메커니즘 구성도

모든 기기에는 고유한 DID(Device ID)와 무선 디바이스의 맥 어드레스를 담고 있는 RFID 태그가 부

착 되어 있다고 가정 한다. 모바일 로봇은 새로운 기기의 RFID 태그의 디바이스 정보를 RFID 리더기로 읽어 들여(①) 홈게이트웨이에 전송 하게 된다(②). 모바일 로봇이 디바이스로부터 읽어 들여 홈게이트웨이에 전송하는 디바이스 정보의 포맷은 그림 4와 같다.

홈게이트웨이는 모바일 로봇에게 받아들인 디바이스 정보에 기기 자신이 속한 홈네트워크를 나타내기 위해 HID(Home gateway ID)를 추가하게 된다.

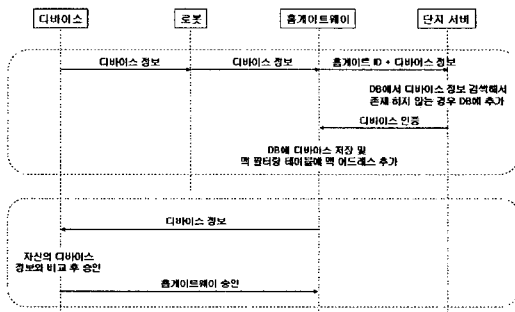


▶▶ 그림 4. 인증 데이터 포맷

그리고 홈게이트웨이는 다른 홈네트워크에 이와 같은 디바이스가 등록이 되었는지의 여부를 확인하기 위해서 단지 서버에게 HID가 덧붙여진 디바이스 정보를 전송 한다.(③) 단지 서버는 데이터베이스에서 이 정보와 일치하는 기기가 있는지를 검사하게 되고 (④) 다른 홈네트워크에도 속하지 않은 기기임이 확인되면 해당 홈게이트웨이에게 이 기기가 신규 기기

임을 인증하게 된다.⑤) 홈게이트웨이는 이 기기의 디바이스 정보를 데이터베이스에 저장하고 맥 필터링 테이블에 맥 어드레스를 저장함⑥)으로써 이 기기를 홈게이트웨이에 등록하여 접근이 가능하게 해준다.

이러한 등록 과정을 통하여 홈게이트웨이에서는 해당 기기가 같은 홈네트워크에 속한 디바이스임을 인증하고 접근을 허용하게 되지만 기기에서는 스스로가 접근을 하려는 홈게이트웨이가 맥내 홈게이트웨이인지 다른 홈네트워크의 홈게이트웨이인지를 판별할 수가 없다. 그러므로 홈게이트웨이는 이전 기기 등록 과정에서 모바일 로봇으로부터 수신한 디바이스 정보의 맥 어드레스에 해당하는 기기에게 아이피를 할당하고 연결설정을 요청한 후 그 기기의 디바이스 정보를 전송 하게 된다.⑦) 기기는 자신이 가지고 있는 디바이스 정보와 비교 하여 두 정보가 일치하면 이 홈게이트웨이가 자신이 속해 있는 홈네트워크의 홈게이트웨이임을 인증하게 된다.⑧) 그림 5는 그림 3에 대한 메시지 프로토콜이다.

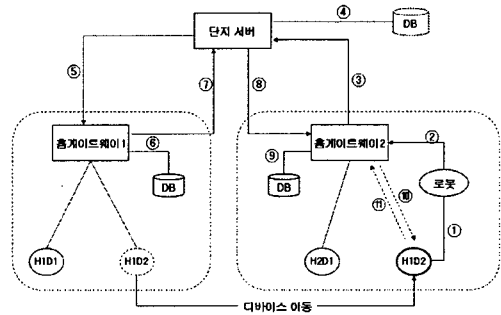


▶▶ 그림 5. 양방향 자동 기기 인증 메시지 프로토콜

2.3. 기기 이동시 자동 기기 인증

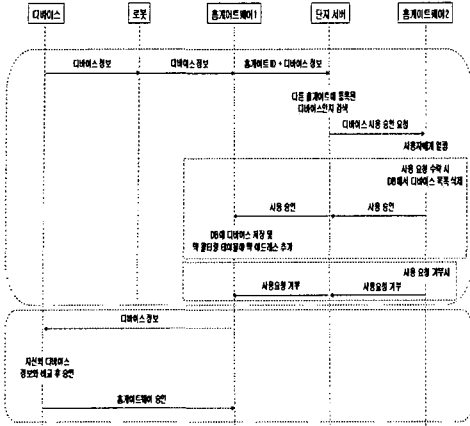
그림 6은 홈네트워크1에서 사용하던 기기를 홈네트워크2로 이동했을 때 인증 처리를 나타내는 메커니즘 구성도이다. 기기에 태그가 부착되어 있다는 가정

은 신규 기기 인증처리 부분과 동일하다.



▶▶ 그림 6. 기기 이동시 양방향 자동 기기 인증 메커니즘 구성도

기기가 홈네트워크1에서 홈네트워크2로 이동을 했을 때 홈게이트웨이2는 이 기기가 신규 기기인 것으로 인식하고 로봇이 기기의 디바이스 정보를 읽어서 홈게이트웨이에 전송하여 단지 서버에서 인증을 받는 절차까지는 동일하다. 그 후에 단지 서버는 데이터베이스에서 동일 정보의 기기가 등록이 되어 있는지 검사를 하게 되고 동일 정보의 기기가 등록이 되어 있다면 그 기기의 홈게이트웨이1에게 홈게이트웨이2에서 기기를 사용하겠다는 요청이 들어 왔음을 알리며 사용 승인을 요청 하게 된다. 홈게이트웨이 1은 맥내의 사용자에게 디바이스가 다른 홈네트워크에서 사용되려 한다는 것을 알리게 되고 사용자가 사용을 허락하면 자신의 데이터베이스와 맥 필터링 테이블에서 해당 기기의 정보를 삭제 후 사용이 승인되었음을 단지서버에게 알리게 된다. 단지 서버는 데이터베이스의 정보에서 해당 기기의 홈게이트웨이를 홈게이트웨이2로 변경 후 홈게이트웨이2에게 사용 승인 메시지를 전송하게 된다. 홈게이트웨이2는 해당 기기를 등록하고 해당 기기에서도 홈게이트웨이2를 인증하여 양방향 인증이 이루어지게 된다. 그림 7은 그림6에 대한 메시지 프로토콜이다.



[8] KETI 기술기획실, "가정용 서비스 로봇", 2004년 12월, 전자부품연구

▶▶ 그림 7. 기기 이동 시 양방향 자동 기기 인증 프로토콜

III. 결론 및 향후계획

본 논문에서는 무선 홈네트워크에서의 기기 인증 방법으로써 모바일 로봇과 RFID를 이용한 양방향 자동 기기 인증 메커니즘을 제안하고 설계하였다. 제안된 인증 메커니즘은 모바일 로봇과 RFID를 이용함으로써 사용자의 편의성을 높여주고, 인증되지 않은 기기에 대한 접근을 원천적으로 차단해준다. 향후 계획으로는 본 논문에서 목표로 하는 인증 메커니즘을 구현하고 더 나아가 홈네트워크에서 사용되는 서비스들의 사용자 권한별 접근에 대한 메커니즘에 대해서도 제안, 구현한다.

■ 참고 문헌 ■

- [1] UPnP Forum, <http://www.upnp.org>
- [2] Homenetwork Security Forum, <http://www.hnsf.org/>
- [3] Wireless LAN, <http://wlan.org/>
- [4] ZigBee Alliance, <http://www.zigbee.org/>
- [5] 강용구, "홈 게이트웨이(Home Gateway) 기술 및 특허 동향", 2004, 한국특허정보원
- [6] "홈네트워크 인증 메커니즘", 2004 한국 전자 통신 연구소
- [7] 이근호, "유비쿼터스 컴퓨팅의 핵심 RFID handbook", 영진